REMARKS

This is meant to be a complete response to the Office Action mailed June 26, 2008. Claims 1, 4, and 20 have been amended to clarify the language within these claims. Specifically, these claims have been amended to illustrate that the unlocking program is ***embedded*** with a password that corresponds to a password protecting a password protected content file that is accessed by an application program. Applicant respectfully submits that the claims, as currently pending, are now in a condition for allowance.

Information Disclosure Statement

In the Office Action dated June 26, 2008, the Examiner indicated that the information disclosure statement filed March 10, 2004 failed to comply with 37 C.F.R. 1.98(a)(1). Applicant respectfully submits that the information disclosure statement filed March 10, 2004 is in full compliance with the rules and statutes and acknowledges the Examiner's statement that it will be placed in the file.

Claim Rejections – 35 U.S.C. § 112

In the Office Action mailed June 26, 2008, the Examiner rejected claims 1, 3-4, and 20-30 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject

matter which applicant regards as an invention. Specifically, the Examiner is concerned with the language in claim 1 reciting "...to at least one password corresponding to the password protecting the content file." In particular, the Examiner would like clarification as to the at least one password and whether the at least one password is different or the same as the password recited in claim 1's preamble. In addition, the Examiner has issue with the language in claim 20 reciting "wherein the at least one password is not revealed to the recipient."

Applicant has amended claims 1 and 20 to clarify the language of these respective claims. In particular, these claims have been amended to more fully clarify that the password automatically supplied to the application program from the unlocking program is the same password that is protecting the password protected content file. Applicant respectfully submits that claims 1 and 20, as amended, and all of the claims which depend therefrom, are now in a condition for allowance. Accordingly, Applicant urges the Examiner to reconsider and withdraw the 35 U.S.C. § 112 rejections of claims 1, 3-4, and 20-30.

Claim Rejection – 35 U.S.C. § 101

In the Office Action dated June 26, 2008, the Examiner rejected claims 20-30 under 35 U.S.C. § 101 stating that the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner believes that claims 20-30 are drawn to a computer-readable medium "that is defined in the specification [sic] can be a communication medium, such as a signal (Page 7, paragraph 16 and 11, paragraph 23)." The Examiner further states that:

> This subject matter is not limited to that which falls within a statutory category of invention because it is not limited to a process, machine, manufacture, or a composition of matter. Instead, it includes a form of energy. Energy does not fall within a statutory category since it is clearly not a series of steps or acts to constitute a process, not a mechanical device or combination of mechanical devices to constitute a machine, not a tangible physical article or object which is some form of matter to be a product and constitute a manufacture, and not a composition of two or more substance to constitute a composition of matter (MPEP 2106).

Applicant respectfully submits that the claims, as currently pending, are directed to statutory subject matter as mandated by 35 U.S.C. § 101. Independent claim 20, and the claims which depend therefrom, specify that the unlocking program is stored on a computer readable medium, which is defined in paragraph [0023] of the currently pending application. As stated in paragraph [0023]:

> The computer readable medium 34 is any type of device, substrate or system ***capable of storing the logic***

> ***constituting the self-executing file 32 and presenting such logic in a format readable by a computer***, such as the owner's computer 12 or the recipient's computer 14. Common examples of computer readable mediums include hard disks, optical disks, floppy disks, tapes, memory, or the like. In the embodiment depicted in Fig. 2, the owner's computer 12 includes the computer readable medium 34 storing the self-executing file 32. The signal path 36 is similar to the signal paths 18, and 22 discussed above. (emphasis added).

Moreover, and as described in paragraph [0016] of the currently pending application:

> The signal paths 18 and 22 can be any suitable communication link which permits electronic communication, such as extra communications systems, intra-computer communications systems, internal buses, local-area networks, wide-area networks, point-to-point shared and dedicated communications, infrared links, microwave links, telephone links, cable TV links, satellite links, radio links, fiber-optic links, cable links and/or any other suitable communication system. It should be understood that signal paths 18 and 22 are shown and described separately herein for the sole purpose of ***clearly illustrating the information being communicated*** between the various components. (emphasis added).

As indicated by the above-mentioned citations to the Specification, the unlocking program recited in independent claim 20 is stored on a computer readable medium that falls within the prescribed subject matter of 35 U.S.C. § 101. A "device, substrate or system capable of storing the logic constituting the self-executing file 32 and presenting such logic in a format readable by a computer," as defined in the Specification of Applicant's

currently pending application, is a machine or a manufacture as recited in 35 U.S.C. § 101. The signal referred to by the Examiner, in fact, refers to a plurality of signal paths, which, as indicated by paragraph [0016], are responsible for transmitting or communicating (rather than storing) the various files (i.e., the password-protected content file and the unlocking program).

As such, Applicant respectfully submits that claims 20-30, as currently pending, are statutory subject matter under 35 U.S.C. § 101. Accordingly, Applicant urges the Examiner to reconsider and withdraw the 35 U.S.C. § 101 rejection of claims 20-30.

Claim Rejections—35 U.S.C. §102(b)

In the Office Action dated June 26, 2008, the Examiner rejected claims 1, 3-4 and 20-27 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,889,860 issued to Eller et al (hereinafter, "Eller"). Applicant, while not conceding on any of the issues addressed in the Office Action mailed June 26, 2008, have amended claims 1 and 20 to expedite the allowance of these claims which are directed to particularly commercially-valuable aspects of the invention.

Applicant's claim 1, as amended, recites a method for distributing a password protected content file without revealing to a recipient a password

that protects the password protected content file. The currently recited method has two steps. First, the unlocking program is distributed to the recipient's computer. The unlocking program has a password ***embedded within*** the unlocking program that corresponds to the password that protects the password protected content file. Second, the password protected content file is distributed to the recipient's computer. The unlocking program automatically supplies a password ***embedded within*** the unlocking program to an application program upon the application program loading the password protected content file wherein the password ***embedded within*** the unlocking program is not revealed to the recipient. Most importantly, security is increased due to the password being embedded within the unlocking program itself, rather than requiring the unlocking program to access an external database to retrieve the password.

Claim 20, as amended, recites an unlocking program for unlocking a password protected content file stored on a computer readable medium and readable by an application program. The password protected content file is locked with a password. The unlocking program is ***embedded with*** a password corresponding to the password locking the password protected content file. The unlocking program also has instructions to automatically supply the password locking the password protected content file to the application program upon the application program loading the password

protected content file. The password locking the password protected content file is never revealed to the recipient. Applicants respectfully submit that the Eller reference does not anticipate claims 1 or 20, as amended, or any of the claims that depend from these claims.

The Eller reference does not teach every element present within Applicant's independent claims 1 or 20, as amended. Rather, the Eller reference teaches a method that includes assigning a password that is specific to the client and transaction, in which the password functions as a decryption key to various informational items (such as a musical score). As stated in the Eller reference:

> The method includes the steps of: establishing a database of information at a server; encrypting at least a portion of the information using a key-based encryption system; in connection with a request by a client, assigning a client-specific key to the client; and ***transmitting the key to the client***. The client-specific key includes some indicia that can be used to identify the client, thereby allowing for monitoring of information use on a client-specific basis...Conveniently such information can be stored in a separate client database and indexed to the key. (Col. 2, Lines 18-25 and Col. 2, Lines 35-37).

In addition, the Eller reference teaches that:

> [The] decryption keys are assigned on a transaction-by-transaction basis. That is, decryption keys are assigned on demand in connection with a transaction involving communication of the protected information from the server to the client. (Col. 2, Lines 53-57).

Upon validation of the client user's payment for the at least partially encrypted information, "the server sends a decryption password and logs the password and other transaction information in its database." (Col. 6, Lines 38-40). After the password is sent from the server, "the client (98) ***then receives the password and stores the password in a password database separate from the downloaded [information]***." (Col. 6, Lines 41-43)(emphasis added).

As indicated above, the Eller reference requires a user client to separately receive a decryption key (i.e., a password) from a server upon the client user successfully tendering payment for the at least partially encrypted information. The separately-received decryption key is then individually stored in an independently-created password database separate from the downloaded information that is encrypted.

As recited in Applicant's amended claims 1 and 20, the password protecting the password protected content file is embedded within the unlocking program. Moreover, this password is automatically supplied to an application program upon the application program loading the password protected content file (rather than requiring the password to be stored in an external password database, as described in the Eller reference).

Applicant respectfully submits that dependent claims 3-4 and 21-30 are also in a condition for allowance, and Applicant hereby reserves the right to continue the prosecution of these claims in a Continuing Application.

As the Eller reference does not teach every element of Applicant's claims 1 or 20, as amended, nor any of the claims that depend therefrom, the Eller reference is not appropriate prior art under 35 U.S.C. § 102(b). Applicant respectfully requests the Examiner to reconsider and withdraw her rejections under 35 U.S.C. § 102(b).

Claim Rejections—35 U.S.C. § 103(a)

In the Office Action dated June 28, 2008, the Examiner rejected claims 28-30 under 35 U.S.C. § 103(a) as being unpatentable over the Eller reference in view of the Examiner's official notice. With respect to claim 28, the Examiner stated the following in support of her rejection:

> As per claim 28, Eller et al. discloses a secured computer system in fig.1 and col. 4, lines 24-64. Eller et al. does not expressly disclose Task Manager program. However, the examiner takes official notice that Task Manager program is well known in the art and every computer has a task manager used to provide information about the processes and program running on a computer, as well as the general status of the computer. Since Eller et al. discloses a secured computer system has computers (servers and clients), it would have been obvious to a person with ordinary skill in the art that Task Manager program is included in the server and client computers of the Eller et al.'s since Task Manager program is well known in the art to

> provide information about the processes and programs running on a computer, as well as the general status of the computer.

Similarly, the Examiner states that claim 29 is rendered obvious because:

> [The] Eller et al. discloses the access program is running from beginning to the end without interruption in fig. 6 and in col. 6, line 61-col. 7, line 39. The examiner takes official notice that an instruction to prevent terminating of a program is common knowledge in the art. It would have been obvious to a person with ordinary skill in the art that there is an instruction to prevent termination of the access software since the access program is able to run from the beginning until the end without interruption with the presence of the task manager (as explained above in claim 28), which is capable of terminate programs.

Finally, the Examiner states that claim 30 is rendered obvious because:

> Eller et al. discloses in col. 2, lines 26-30, '...for example, digital sheet music,...or other subject matter transmittable in digital form". Although Eller et al. does not expressly disclose pdf format, however, the examiner takes official notice that subject matter transmittable in digital form includes pdf format is well known in the art. It would have been obvious to a person with ordinary skill in the art that content file disclosed in Eller et al. includes pdf format since pdf format has been used in the art for over fifteen years and it is well known in the art that the pdf format content file can be digitally transmitted from any application on any computer system.

As discussed above in reference to the 35 U.S.C. § 102(b) rejections, claim 20, of which claims 28-30 depend, has been amended to clarify that

the password protecting the password protected content file is embedded within the unlocking program itself. This is in stark contrast to the method recited in the Eller reference, in which a server is required to separately transmit a decryption key to a client user that is subsequently stored in an independent password database on the client user's computer.

By embedding the password within the unlocking program itself, as recited in Applicant's currently pending claims, there is no need for the unlocking program to access an external database to retrieve a password that corresponds to the password protecting a password protected content file. This lack of a retrieval from an external password database increases the security as the end user will not know the location or have ability to gain access to the password protecting the password protected content file. In light of the amendments to claim 20, Applicant respectfully requests reconsideration and withdrawal of the rejections set forth above as applicable to claims 28-30.

CONCLUSION

This is meant to be a complete response to the Office Action mailed June 26, 2008. Applicants respectfully submit that each and every rejection has been overcome. Favorable action is respectfully solicited.

Should the Examiner have any questions regarding this Amendment, or the remarks contained herein, Applicants' attorney would welcome the opportunity to discuss such matters with the Examiner.

Respectfully submitted,

Marc Brockhaus

Marc A. Brockhaus
Registration Number 40,923
DUNLAP CODDING, P.C.
Customer No. 30589
P.O. Box 16370
Oklahoma City, Oklahoma 73113
Telephone:(405) 607-8600
Facsimile:(405) 607-8686

Attorney for Applicant